The Quest for the Effective Protection of the Right to Privacy

Wisman, T.H.A.

2019

document version
Publisher's PDF, also known as Version of record

Chapter VII
Conclusion

The right to privacy and data protection legislation

As revealed in the two case studies of this thesis, it is the data protection legislation that the Commission relies on in its policy and rule-making activities on mandatory IoT systems. As established in Chapter 3, data protection legislation can offer guidance in establishing certain safeguards and principles such as data minimisation and purpose limitation which have the potential to prohibit the legislator from equipping these systems with unnecessary surveillance features — what is coined as the prohibitive potential. Data protection law is limited in scope and only offers this potential with regard to features involving the processing of personal data. It is inadequate to address other features of IoT systems, such as actuators and sensors that can be remotely turned on or off. More pressing, however, is the point that data protection law is commonly relied on in transparent relationships which are usually entered into voluntarily.

The transparency requirement follows from a number of data protection rules, such as the duty of the controller to inform the data subject about the processing and the subjective rights (access rights) for the data subject. The mandatory installation of IoT systems in the private sphere of citizens is controversial and politically sensitive as it can take place voluntarily, involuntarily or even unknowingly. Moreover, these systems serve a broad plethora of interests, most of which are at odds with the interests of citizens in informational privacy. The current information society, in which these systems function, is characterised by the opacity of data processing operations. This was, once again, demonstrated by the upheaval caused by the revelations about the collaboration between Facebook and Cambridge Analytica.

Another problem with data protection law is that it leaves the interpretation and application of principles with prohibitive potential to the data controller. Furthermore, data protection law does not apply to ESOs, which are the parties developing the technical rules for IoT systems. A final objection to the excessive reliance on data protection law is that its application is not likely to question the necessity of the initial recording and collection of data by IoT systems. Data protection law, in isolation from the right to privacy, is ill-suited in mediating the conflict-ridden relationship between the legislature and the Commission on the one hand – and in the slipstream of the latter also industry – and the interests of citizens in the effective protection of the right to respect for their private life and home on the other.

The fluidity of the concept of privacy is reflected in the creativity it allows the courts in interpreting and applying it to technological challenges raised by the developments in the information society. Although far from perfect, the right to privacy has been a steady and

reliable source for judicial innovations directed at the protection of citizens against the power of the state or industry. Taking the conflicting interests involved in the architectural choices regarding IoT systems as a starting point, the right to privacy is well-suited to engage in the required mediation of these interests. Moreover, the scope of the right covers all features of IoT systems, those that concern the processing of personal data, but also sensors and actuators that can be controlled remotely.

The analysis of the case law of the ECtHR and the CJEU suggest a number of factors which contribute to the assessment of the severity of the interference, as well as to the impact assessment of the Commission. Three factors are distinguished in this thesis of which the first two concern the processing of personal data only. These are the context of the processing, the nature of the data and the potential future violations. Both the ECtHR and the CJEU have demonstrated to be susceptible to the extent to which a measure facilitates further interferences in the future. This factor can be coined the potential future violations, in which the potential future use of data and systems can be assessed. There lies a duty with the legislature to assess the impact of IoT systems beyond their initial purpose and functioning and critically evaluate what can be, instead of limiting itself to what is. Some of the surveillance features of IoT systems are self-evident, such as the communication of detailed usage of electricity data by smart meters. Others are more complicated to discover as the features seem innocuous at first sight, only to reveal their surveillance and control potential upon closer scrutiny. One example of this is the microphone of eCall which is intended to facilitate communication between the motorist and a PSAP, but which can be used to eavesdrop on conversations in the car. One control feature which requires a high level of understanding of technology is the possibility to use the eCall system to shut down cars at a distance.

The two other factors apply primarily to the processing of personal data and concern the context of the processing and the nature of the data. The context can be helpful in analysing and establishing the relevant factors which determine the severity of the interference caused by the installation of IoT systems. First of all, it is in the nature of the IoT vision that the obligation to install these devices will affect virtually all citizens within the EU. Second, their installation does not take place on the basis of consent. It is a system which penetrates into the private sphere of citizens on the basis of statutory force. Any subsequent surveillance feature these devices are equipped with will be a feature that affects the lives of all citizens. An uncurbed surveillance potential could subject aspects of citizens' private lives to permanent recording and collection of data and basically amount to an obligation to live online, with all the ramifications one can think of. In the Commission's communications on data in the future economy, this data will be used for a multitude of purposes. If the IoT systems discussed in this thesis are used for these purposes it implies that, except for some applications in business relationships, the data is used without consent of the citizens. IoT systems have the potential to animate private spheres and properties and to turn them against inhabitants and users, consequently eroding not just their right to privacy, but their very freedom, or in Brandeis words, their 'personal security'.

A number of requirements follow from the right to privacy. In view of the near-continental implications for the right to privacy related to the architectural choices at hand, the EU legislature enjoys a narrow margin of appreciation when it comes to design features which interfere with the right to private life and the home. The requirement of necessity embedded in the proportionality test – used to establish the lesser restrictive means to attain a goal – should be taken into account already in the first elaborations on system design. This test allows to 'smoke out unacceptable motives' guiding the system's design.[1] It follows from this test that IoT systems should not enable centralised storage of data when the officially stated goal of the installation can be pursued through decentralised storage. By restricting the functions of IoT systems to what is necessary their surveillance and control potential can be adequately addressed. This element of the proportionality test also links to the doctrine of positive obligations where the EU legislature should 'minimise, as far as possible, the interference with these rights, by trying to find alternative solutions and by generally seeking to achieve their aims in the least onerous way as regards human rights'.[2] The reliance on the power of the EU legislature to force the installation of IoT systems in the private sphere, places the burden of responsibility for the avoidance, or alternatively minimisation, of interference(s) following from this, firmly with the EU institutions.[3]

If the interference, or the risk of interference, cannot be avoided in the design, proportionality in the strict sense has to be tested by balancing the interests at stake against the right to privacy. The functions which create (risk of) interferences should have a clear and foreseeable basis in the legislative act introducing the system. Adequate safeguards should be adopted to address, amongst others, risks of abuse. If the exploitation of these functions facilitates mass surveillance practices it is unlikely that the right to privacy will be outbalanced by the interests of other parties. Drawing up extensive laws which would allow these practices does not change this conclusion, as was demonstrated in the judgments of the CJEU on data retention.[4] An IoT data retention regime exposes citizens' lives to arbitrary interferences by public authorities, businesses and malevolent parties. The perspective of the mandatory installation of surveillance equipment, which records and communicates detailed data to a central server where it is mined for a multitude of purposes, compromises the essence of the right to privacy. Even if these purposes are meticulously set out in data protection legislation, it would not change the conclusion that this would affect everybody on an unconditional basis. The rationale of human rights generally and Article 8(2) ECHR particularly takes freedom as the rule and interference as the exception. This requirement follows from the texts of the ECHR and the case law of both courts.[5] The right to privacy is

[1] Eva Brems and Laurens Lavrysen, '"Don't Use a Sledgehammer to Crack a Nut": Less Restrictive Means in the Case Law of the European Court of Human Rights' [2015] 15/1 HRLRev 139, 143.

[2] Hatton and Others v The United Kingdom Application no. 36022/97 (ECtHR 2 October 2001) para 86.

[3] This is also consistent with other case law from the ECtHR. See López Ostra v Spain App no 16798/90 (ECtHR, 9 December 1994) para 55.

[4] Joined cases C-203/15 and C-698/15 Tele2 Sverige EU:C:2016:970.

[5] Article 8(2) ECHR explicitly mentions the exceptional character of the interference. 'There shall be no interference (…) except such as is (…).This requirement was also confirmed by the CJEU in Tele2 Sverige,

the rule, the interference should be the exception. The mandatory installation of IoT systems recording and retaining data indiscriminately turns the interference into the rule.

Both the right to privacy and data protection legislation work with the notion of necessity and offer requirements which can be used address the surveillance potential of IoT systems. Moreover, they can complement each other as is demonstrated in the case law of both the CJEU as well as the ECtHR. Data protection legislation, however, does not address the control potential of these systems. Together these rights, taken seriously, could inform an IoT policy in which architectural choices are taken by the legislature with their protection as a priority.

The conflicting roles of the Commission

One of the problems of the Commission's role in the IoT policy and rule-making process lies in its performance of two, at times irreconcilable, roles. On the one hand, the Commission is a policy entrepreneur which brings together public and private parties in the policy fields pertaining to the mandatory systems, in order to align their respective interests and contribute to the establishment and the functioning of the digital single market. In this process, the Commission is sensitive to the wishes of the more powerful parties, because it is dependent upon them for the success of the policy it formulates. Such dependency puts it in a difficult position with regard to its second role, that of the guardian of fundamental rights. There, the Commission must see to the effective protection of fundamental rights in its communications, legislative proposals and quasi-legislative activities. In this role, taking fundamental rights seriously is likely to lead to conflicts with its policy partners.

In the pre-legislative phase the Commission's ambivalence helps to explain why it focuses in its communications on data protection law, whilst meaningful considerations on the right to privacy are absent.[6] Data protection legislation is elaborated on, but the prohibitive potential of data protection legislation is not discussed. The contours that become visible in these documents is one in which data security and procedural rules on the use of data are prominent, which results in what one might view as the Commission's *data protection-light* approach. One returning phenomenon in these documents is the use of data on a mass scale for multitude of purposes, including those conflicting with the interests of citizens, implicitly rejecting the principle of purpose limitation. This amounts to a radical departure from the original conception of data protection, discarding the legal fundament without which the processing of personal data cannot be justified.

The stakeholders the Commission is involved with in its role as executive governing IoT-policy are typically either economic operators or public authorities that have an interest in the recording and dissemination of data by (mandatory) IoT systems and, thus, a loose

---

where it held that a legal basis which allows restrictions on the scope of a fundamental right should be interpreted strictly and cannot allow the exception to become the rule. Tele2 Sverige and Watson (n 4) para 89.

[6] See Chapter 4, section 2.

interpretation of privacy and data protection legislation. A strict interpretation and application implies that the personal data processed is limited to the strict minimum necessary to attain the stated policy goal. This would be energy efficiency in the case of smart meters and road safety in the case of eCall. Such limitation of the personal data processed implies the reduction of commercial stakeholders' incentive to participate and cooperate in the implementation of this policy. For the Commission the loose interpretation and application of privacy and data protection law is conducive towards realising concrete policy goals; it is even likely to contribute to building closer ties with its policy partners. This helps to explain the contradiction between the Commission's rhetoric on its supposed quest for the most effective protection of fundamental rights, and the data protection-light approach that it takes in its policy and rule-making activities regarding smart meters and eCall.

In the legislative phase, the Commission interprets and applies the right to privacy and data protection at various points, the most important of which is the impact assessment. One of the aims of this assessment is to establish the impact on fundamental rights, already in the early stages of the development of a proposal. The next step is to address this impact accordingly, in line with the case law of the CJEU and ECtHR, ultimately leading to a proposal which respects the Charter of Fundamental Rights. The impact assessment in theory provides the fundamental rights groundwork for a legislative proposal. The Commission produced a rich body of communications, reports and guidelines in which it has taken an ambitious approach to the protection of fundamental rights, where in its own words the EU should fulfil an exemplary role by making the Charter rights 'as effective as possible'.[7]

Even though such a systematic and pragmatic approach should be welcomed, a number of pitfalls have been identified. First, in the impact assessment the legislative act will be taken as a starting point to assess the IoT system. This allows the Commission officials to sidestep difficult questions that might be raised if the assessment included unforeseen scenarios in which these systems can be used. Potential privacy violations which consist of the secondary use of IoT systems should be part of the impact assessment. Second, the execution of this impact assessment takes place after the Commission has mapped out the policy and established its main features. Moreover, the extent to which the impact assessment will recognise design choices for IoT systems as a matter of fundamental rights is dependent upon the Commission employees' conception of fundamental rights, which in turn is likely to be affected by the data protection-light rhetoric, which appears to be ever-present in the Commission's communications. This raises the question whether the impact assessment allows for genuine proofing of fundamental rights, or is it destined to be a mere box-ticking activity.

There is another pitfall which is linked with the quasi-legislative phase. The focus of the impact assessment is on the main legislative act, while the sting can be in the delegated or implementing acts. Here, the ESOs at the request of the Commission develop technical rules the system should abide by. The probability that these rules will amount to violations of the

[7] Commission, 'Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union'(Communication from the Commission) COM (2010) 573 final 3.

right to privacy increases if the Commission does not set boundaries in its request. There are two constitutional limits for the legislature. There is the non-delegation doctrine which instructs the Commission when it adopts 'non-legislative acts of general application to supplement or amend certain non-essential elements of the legislative act' and that 'the essential elements of the area shall be reserved for the legislative act'.[8] This imposes a duty on the Commission to refrain from adopting delegated acts which contain essential elements. What qualifies as essential is not merely subjective and, according to the CJEU, it also depends upon 'objective factors amenable to judicial review'.[9] The CJEU established two such factors consisting in political choices for the legislature and when decisions concern fundamental rights.[10] These factors link the competence of the Commission in the quasi-legislative phase back to the ultimate aim of the impact assessment: to guarantee that the legislative proposal respects the Charter. In order to pursue the most effective protection of the rights enshrined in the Charter the Commission should propose rules in the legislative act setting the limits for its own work in the quasi-legislative phase. These rules can also contribute to the EU legislature acting in line with the second constitutional limit, the specificity principle, which provides that the 'objectives, content, scope and duration of the delegated power shall be explicitly defined in the legislative acts'. The legislature has a duty — stemming from the specificity principle and the non-delegation doctrine — to take the essential elements of the act into account whilst defining the details of the power conferred on the Commission. The definition of the conferred powers needs to take into account the interferences as well as risk of interferences with the right to privacy posed by the installation of the IoT system. It should also ensure that the requirements following from the Charter are respected. This is also in line with the foreseeability requirement. The legislature has the duty to set the *essential elements of design*. These contain the type and content of safeguards addressing the elements of IoT system design which can negatively impact fundamental rights and which concern opposing interests between industry and citizens. This duty for the legislature can be seen as the hinge between the role of the Commission in the impact assessment and the role of the Commission in the quasi-legislative phase. Ideally, the impact assessment would prepare the ground for the legislature and assist it in establishing the essential elements of IoT system design in the legislative act, adequately addressing the surveillance and control potential of the system and ensuring the effective protection of the right to privacy. If the impact assessment does not establish any impact on fundamental rights, it is unlikely that the EU legislature will identify a problem in provisions on implementing and delegated powers in the legislative proposal. This gives rise to the same criticism raised above with respect to the impact assessment: the work of the Commission builds on its misconception of data protection.

If these elements are not set in the legislative act and this silence is perpetuated in the mandate the Commission issues to ESOs, this mandate will not set limits with respect to

[8] This duty also applies to the implementing acts. See Chapter 4, section 4.1.

[9] C-355/10 Parliament v Council EU:C:2012:516, paras 67, 68.

[10] Ibid para 77. Maarten den Heijer and Eljalill Tauschinsky, 'Where Human Rights Meet Administrative Law: Essential Elements and Limits to Delegation' (2013) 9 European Constitutional Law Review 513, 519.

fundamental rights which have to be respected whilst drafting the standards. This mandate is in fact a contract and the Commission failing to address respect for fundamental rights in this capacity means its bargaining away Europe's hard-won human rights heritage. This would mean private parties enjoy discretion on essential elements of the legislative act, involving architectural decisions on the surveillance and control potential of the system. Thereby, it should be kept in mind that the constituency of ESOs consists of representatives of a profit-driven industry with an interest in personal data as an economic asset. It is, however, unlikely for the Commission to adopt requirements in the mandate if these are absent in the main legislative act. Even if the Commission adopted them, the ESOs could refuse to accept the mandate.[11] The legal status of a mandate is a contract, which is more accurately defined as a 'request' in the Standardisation Regulation, and ESOs are free to refuse this. The formal discretion of the Commission to determine the requirements and policy objectives, thus, finds its limits in its dependency on the ESOs in fulfilling their task.[12] ESOs have a monopoly position and can simply veto requirements viewed as too strict and which do not follow from the legislative act. Setting out the requirements in the legislative act provides the Commission with a clear framework for its mandate and a strong position within the negotiation process with the ESOs.

Officially the Commission oversees the development of the standard, however, commentators criticise the Commission for lacking expertise, resources and willingness to attend the meetings of the ESOs as observers.[13] There is a gap between the expertise of the Commission compared to that of the ESOs, which is even wider in relation to the EP and the Council. Problems born out of this expertise asymmetry in this principal-agent relationship are agency shirking and slippage.[14] Agency shirking refers to the behaviour of the agent, in this case the ESOs and their lack of effort to meet requirements which do not serve their interests. Agency slippage refers to the principal, in this case the Commission and its inability to effectively see to the ESOs meeting the requirements. The Commission's dependence on the ESOs and its lack of expertise, resources and willingness undermine its ambition to guard the effective protection of fundamental rights in the case of smart meters and eCall.

[11] Article 10(3) of Council Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council [2012] OJ L 316/12.

[12] Christian Frankel and Erik Højberg, 'The constitution of a transnational policy field: negotiating the EU internal market for products' (2007) 14 Journal of European Public Policy 108, 109.

[13] Harm Schepel, The Constitution of Private Governance: Product Standards in the Regulation of Integrating Markets (1st edition, Hart Publishing 2005) 243.

[14] Michelle Egan, 'Regulatory strategies, delegation and European market integration' (1998) 5 Journal of European Public Policy 485, 489.

The case study of the smart meter and the eCall system

The case studies into the mandatory IoT systems followed a somewhat divergent approach due to the particularities of both cases.

The policy and rule-making process regarding the functionalities of the smart meter consisted of negotiations between the Commission and Member State representatives responsible for energy. There are no traces of any deliberations on fundamental rights, or data protection law, in the document in which the privacy infringing functions of smart meters were established.[15] Directive 2012/27 does not provide any privacy infringing functions, and inferring these functions from the Directive requires adequate knowledge of the policy field and extensive further analysis. The technical description of the functions, in any case, cannot satisfy the standards of foreseeability which follow from ECtHR case law. This, in turn, also reveals that the EU legislature's approach on the smart meter legislation violates the specificity principle.

The silence on privacy infringing functions in the energy directives can be explained by the Commission not conceiving them as such. This is also evidenced in the explanatory memoranda of Directive 2006/32/EC, Directive 2009/72/EC and Directive 2012/27/EU, which share a common characteristic: not a single word is dedicated to either fundamental rights or data protection legislation. The groundwork for this awkward silence was laid in the impact assessments executed prior to the proposal of Directive 2009/72/EC and Directive 2012/27/EU: neither of them addressed the right to privacy or data protection law. The awkwardness of this silence increased by the fact that both the Article 29 WP and the EG2 have highlighted the importance of architectural choices of smart meter design, in particular the choice between centralised and decentralised storage of detailed data, where both recommended decentralised storage.[16] The Commission has ignored these recommendations and has not justified its choice for centralised storage, despite the apparent conflict with its proclaimed fundamental rights ambitions. The preference for centralised storage is at odds with the availability of lesser restrictive means, which is a requirement unequivocally following from both the right to privacy and data protection legislation separate and in conjunction. The Commission's choice goes against the imperative of the fundamental rights framework. Moreover, the recognition that these architectural choices concern the essential elements of the area reserved for the legislature would force it to defer this choice back to the Council and EP.

The need to make fundamental choices has also been ignored by the Commission in the mandate it offered to the ESOs indicating only that data protection deliverables should take into account applicable legal requirements concerning the confidentiality of personal data

[15] EU Commission Information Society and Media Directorate-General and Energy Directorate-General, 'A joint contribution of DG ENER and DG INFSO towards the Digital Agenda, Action 73: Set of common functional requirements of the Smart Meter' (Full Report, The Publications Office of the European Union 2011).
[16] See Chapter 5.

protected under Directive 95/46/EC and Directive 2002/58/EC'. [17] The focus on confidentiality as a form of data security confirms the Commission's neglect of principles with prohibitive potential, the application of which could lead to the minimising of collection and storage on the meter, thus, facilitating informational control of meter holders, i.e. the citizens. By remaining silent on these issues, the Commission effectively leaves space to ESOs to take decisions with fundamental implications for power relations between households on the one side and government and industry on the other. The Commission's silence is understandable if the smart meter architecture is viewed through the prism of data protection-light. If one, however, looks at it through the lens of ECtHR and CJEU case law it becomes clear that the design choices for the smart meter can be considered an historical error with implications for the entire EU. The intrusive potential which follows from the monitoring and controlling features of the smart meter strikes at the heart of personal freedom and permanently breaches the right to respect for the home that is fundamental to people's personal security and well-being.

If the European roads are transformed into an internet of things, than the eCall system is what the Commission aims to tag cars with in order to make motorists surf in this new technological paradigm. In four consecutive communications the Commission, hinted at the mandatory introduction of eCall in various forms: the possibilities to adopt legislation mandating 'advanced safety systems';[18] 'in case the eCall roll-out fails [the Commission is] to (…) consider further measures';[19] if the automotive industry failed to accept a 'voluntary agreement of introducing an eCall in-vehicle device [the Commission will] propose further measures'[20] and 'setting up a regulatory framework for deploying eCall'.[21] This sheds new light on the Commission's carrot and stick tactics, in which it demonstrated its willingness to beat the mule into eating the carrot. Despite its own findings that industry struggled 'with a non-obvious business case and reluctant consumers' and the public sector was 'not (or not sufficiently) aware of the potential of ITS to help achieve policy objectives', [22] the

[17] Commission, 'Standardisation mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability' (Enterprise and Industry Directorate-General , Consultation date: 21 January 2009) M/441 EN.

[18] Commission, 'Information and Communications Technologies for Safe and Intelligent Vehicles' (Communication from the Commission to the Council and the European Parliament) COM (2003) 542 final 13.

[19] Commission, 'The 2nd eSafety Communication: Bringing eCall to Citizens' (Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions) COM (2005) 431 final 10.

[20] Commission, 'Bringing eCall back on track – Action Plan (3rd eSafety Communication)' (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions) COM (2006) 723 final 8-9.

[21] Commission, 'eCall: Time for Deployment' (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions) COM (2009) 434 final 3.

[22] Commission, 'Impact Assessment accompanying the Communication from the Commission Action plan for the deployment of Intelligent Transport Systems in Europe and the Proposal for a Directive of the European Parliament and of the Council lying down the Framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other transport modes' (Commission Staff Working Document) SEC (2008) 3083, 47.

Commission displayed great tenacity in realising the adoption of eCall, either voluntary or compulsory. The interests of the stakeholders involved and the variety of purposes pursued by the installation of eCall raise the question what the implications of these envisioned applications are for the design of the mandatory system. The majority of these applications do not fall under the purpose of safety used to justify the mandatory installation, yet they do influence the design of the system that is forced into the cars of all citizens.

This lack of clarity surrounding the purposes served by the installation of eCall and the system's relation to ITS, is perpetuated in the ITS Directive and the eCall Regulation. The ITS Directive introduced 'the harmonised provision for an interoperable EU-wide eCall' as a priority action, without a definition of the system.[23] The five delegated regulations which were adopted on the basis of this Directive and included matters such as the 'EU-wide real-time traffic information services' do raise questions if, and if so, how these relate to the functioning of eCall. The eCall Regulation introduces seven distinct terms for eCall-services and six distinct terms for eCall-systems, without any of these recurring in the definitions. The result is that this regulation is as puzzling to read as a pirates' treasure map and that the implications are hard to grasp for a layman. The eCall Regulation does define the '112-based eCall in-vehicle system' as an 'emergency system, comprising in-vehicle equipment and the means to trigger, manage and enact the eCall transmission' and the 'eCall' as an in-vehicle emergency call to 112'. The obligation to install eCall is linked to its emergency-related function as opposed to the added value services that build on it.[24] Added value services and the open-access platform are introduced in Recital 15, yet there are no further provisions elaborating on how they relate to the 112 system. Definitions of added value services and the 'open-access platform' are not provided. The text of the Regulation also remains silent on definitions for added value services and 'future in-vehicle applications and services'. A legal vacuum is, thus, created with respect to these services and the functioning of the mandatory in-vehicle system. Such silence is staggering in the face of the potential extreme consequences outside emergency situations. The use of eCall in emergency situations, in the hypothetical scenario that all cars are already equipped with it, directly concerns only 0,002869% of EU motorists, in contrast to the system's potential for secondary use which can affect all motorists.[25] This silence cloaks the fact that secondary use of a system which is forced into private property under the banner of saving lives, for a plethora of interests which do not necessarily align with the owner of the vehicle, is politically controversial, legally questionable and morally loose.

The impact assessments accompanying the ITS Directive, the eCall Recommendation and the eCall Regulation demonstrate how the Commission continues its quest for the effective protection of the right to privacy by viewing it through the prism of data protection-light. The one paragraph on fundamental rights that is fumbled in the impact assessment of the ITS Directive, states that attention will be paid to individual privacy. No strands of thought from

[23] Article 3(d) Directive 2010/40/EU.
[24] Article 3(1)(2) Regulation 2015/758/EU.
[25] See Chapter 6.

the case law of the CJEU and ECtHR are to be found, however, which explains that the initial recording and collection of data are not recognised as an interference and subsequently not tested against the requirements which follow from Article 52 Charter. Privacy and data protection are commonly addressed in terms of 'data security, privacy and liability', and elaborations on these categories are devoid of any substantive reasoning. The impact assessments are silent on architectural choices with implications for fundamental rights. Before any useful assessment of the necessity of eCall or its design can take place, the problem the system is supposed to solve should first be established. Even this task, which is the first concern in the execution of the impact assessment, is not performed properly by the Commission. The Commission frames the problem as the slow and fragmented uptake of ITS, whilst ITS is an umbrella term for almost everything involving ICT and cars.[26] This does not qualify as a well-described problem. An accurate description of the problem is essential within the fundamental rights impact assessment in order to establish if and to what extent an interference with fundamental rights is justified, as a precondition for setting objectives and considering different policy options, as well as for outlining safeguards mitigating the impact on fundamental rights. Testing proportionality requires the assessment of the relation between the ends and the means. If the Commission wishes to be faithful to its own fundamental rights policy declaration, at the very least it should clearly identify the ends for which it proposes certain measures. It is unfortunate that there is no acknowledgement by the Commission of the great potential for fundamental rights violations. The lack of attention to the design of the system in the impact assessments and the explanatory memoranda, given the privacy concerns raised by the Article 29 Working Party and recognised in the impact assessment of the ITS Directive in 2008, qualifies the Commission's approach as wilfully negligent. Once again, a contrast can be seen between the Commission's rhetoric and practice.

The (risks of) interferences with the right to private life raised by the eCall system can be divided into two categories. There is the exploitability of its communication technologies, sensors and actuators, which allow for targeted interferences, such as eavesdropping and remotely shutting down the car.[27] The biggest (risks of) interferences, however, follow from the ambition to use the 112 system to provide added value services. The Commission identified privacy threats following from these services, such as unauthorised access to personal data, re-use of personal data beyond the legally defined purpose and excessive processing.[28] Re-use for a legally defined purpose, nonetheless, might just as well pose a threat to motorists' privacy. More troublesome is the envisioned use described in the latest Commission report and announced on the ACEA website.[29] The claims made in this report suggest that data protection law only applies to the use of data and not to the initial collection. Although demonstrably wrong, this application of data protection law is not out of tune with the interpretation and application of data protection legislation by the Commission, as

[26] SEC (2008) 3083 (n 22) 12.

[27] Council of the European Union, 'ENLETS Work programme 2014-2020: European Network of Law Enforcement Technology Services' (Doc 17365/13, The Publications Office of the European Union 2013) 5.

[28] Stefan Eisses, Tom van de Ven and Alexandre Fievée, 'ITS Action Plan: ITS & Personal Data Protection' (Final Report, European Commission DG Mobility and Transport 2012) 6.

[29] See <http://cardatafacts.eu/> accessed 7 June 2018.

analysed in this research. The failure to question the necessity of the initial recording and collection of data by the IoT systems is typical of the Commission's approach, even though this approach is usually not made explicit. This can be explained by the fact that this report carries a Commission stamp, but was prepared by TRL. This demonstrates in unearthing terms what the Commission meant when it indicated that automotive industry was interested in eCall as a 'platform to offer added value services to boost their business'.[30]

Both the ITS Directive and the eCall Regulation confer powers to the Commission, without instructions on privacy or data protection. The ITS Directive establishes 'Rules on privacy, security and re-use of information' for Member States. These rules, however, mainly concern the duty for Member States to protect data against unlawful access, alteration or loss, i.e. data security. The eCall Regulation only addresses car manufacturers, not the Commission. Moreover, the instructions contain referral to principles without specifying or applying them. In both the ITS Directive and the eCall Regulation, the specificity principle and the requirement of foreseeability are not respected in relation to added value services. The decisions taken by the Commission and the standards developed by ESOs have implications for the respect for the right to privacy and the protection of personal data and, as such, concern essential elements which are the preserve of the EU legislature. This point has also been stressed by the EDPS.[31] Despite recommendations of the EDPS and the DG Mobility and Transport on the potential for PETs to shield privacy of motorists, similar to the solutions proposed by Jacobs,[32] there is no trace of a follow-up on this issue by the Commission. The EDPS's warnings that the silence on added value services would result in the creation of a 'legal loophole' fell on deaf ears.

The link between the mandate and the relevant legislative requirements established in the Standardisation Regulation is absent. Mandate M/453 was issued in 2009, long before the drafting of the eCall Regulation, but just one and a half month following the Commission communication 'eCall: Time for Deployment'. eCall is not mentioned in this mandate. It was aimed at supporting the interoperability of C-ITS systems.[33] The standards were developed on the basis of this mandate and were subsequently adopted in the eCall Regulation. Thereby these documents attained statutory power,[34] yet these documents can only be accessed after paying a substantial fee. Furthermore, they are written in complex technical language almost incomprehensible to a layman. In short, the adoption of these standards significantly undermines the rule of law in the EU.

[30] COM (2009) 434 (n 21) 6.

[31] EDPS 2010, C 47/10, para 24.

[32] Bart Jacobs, 'Architecture Is Politics: Security and Privacy Issues in Transport and Beyond' in Serge Gutwirth and others (eds), *Data Protection in a Profiled World* (Springer 2010) 291.

[33] European Commission, 'Standardisation Mandate addressed to CEN, CENELEC and ETSI in the field of Information and Communication Technologies to support the interoperability of Co-operative systems for Intelligent Transport in the European Community'(DG ENTR/D4 M/453 EN , European Union 2009).

[34] This can be compared to smart grids: Robin A Hoenkamp, Adrienne JC de Moor- van Vugt and George B Huitema,'Law and standards: Safeguarding societal interests in smart grids' in Ronald Leenes and Eleni Kosta (ed), Bridging distances in technology and regulation (Wolf Legal Publishers 2013) 117.

Analysis of eCall policy exposes a public-private effort to transform private cars into beacons of personal data which are subsequently utilised for the good of government and commerce. Statutory force has been used as a crowbar to install a system which serves a corporate agenda, leaving the impression of an unholy union of governmental and commercial interests.

Concluding thoughts

Freedom and autonomy are two important values protected by the right to privacy. Data protection legislation is sometimes compared with environmental law, because it seeks to remedy the harmful external effects of the processing of personal data. Data was described in the Economist as 'the new oil' comparing data centres to drill platforms.[35] Data can be seen as a new raw material for the functioning of a variety of processes. The more personal this data is the more extensive is the 'pollution' that follows from it. Only the 'pollution' here consists in the negative external effects of data processing on the liberty and autonomy of the people concerned. The data centres depend on raw material to perform their operations on. The mandatory IoT systems can be seen as drill platforms which drill for data. The difference between a system that respects privacy and one that does not is a difference between a system harming freedom and autonomy and one that does not do so.

This difference in harm needs to be multiplied by the number of systems that are installed across the EU. Although impossible to express in numbers, it gives an idea of the implications at stake for the architectural choices at hand. These implications are not recognised in any of the documents produced by the Commission in the course of the policies and legislation assessed in this thesis. Invoking the right to privacy allows challenging the compulsory installation of invasive devices in ones' private environment. It also demands a critical evaluation of the necessity of the introduction of such technologies and a balancing of the rights and interests at stake. No such evaluation has been conducted. Moreover, the Commission has failed to state the exact problem it seeks to solve through the deployment of the relevant systems.

How did the Commission succeed in brushing of the responsibility it took upon with much bravado, even claiming that the post-Lisbon status of the Charter would result in a 'fundamental rights reflex' in its departments responsible for drawing up proposals and acts?[36] How can the Commission justify the fact it does not even recognise that the mandatory installation of smart meters and eCall is a fundamental rights issue? The answer lies in the data protection-light approach it takes to privacy concerns. With this approach the Commission neglects all rules which have a prohibitive potential and shifts the focus to the sharing of data according to a set of rules, rather than preventing the latter or putting the data subject in control. The Commission pays lip service to data protection and privacy, but it

[35] 'Data is giving rise to a new economy' (Economist, 6 May 2017) <https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy> accessed 7 June 2018.

[36] COM (2010) 573 (n 7).

stays silent on rules that would get in the way of the data processing schemes of the stakeholders involved in IoT policy. The data protection-light approach is the foundation on which the Commission constructs data protection issues in all phases of policy and rule-making and allows it to reduce human rights concerns to easy to digest technical issues for the major stakeholders involved. The Commission uses the language of data protection to justify data dispossession.

Decisions about system design take place outside the democratic arena without meaningful oversight in a homogeneous environment of technical experts serving the business community and overzealous public servants seeking to expand the governmental sphere of influence. These decisions are inspired by a mix of government and commercial considerations that benefit the few, while its potential drawbacks concern all citizens in EU Member States. The mandatory installation of invasive IoT systems is presented as the solution to a range of societal issues. This narrative follows the narrow interests of these few powerful well-organised groups and is founded on a monistic materialist view of society lacking a critical review of the IoT systems and their effects. The stakeholders they represent reap the benefits from the data drilled by IoT systems leaving citizens bereft of their privacy and freedom. This will increase the a-symmetry already present in the power relations in which they are deployed. IoT policy in which certain private aspects of everyday life are subjected to an intense surveillance regime mark the departure from the founding values of the EU.[37] Democracy means respect for a pluralist society and the imposition of this monistic view on society goes against the very nature of this distinctive feature of the European project. Pluralist society will not be respected by applying 'data protection principles in the private sphere'.[38] IoT policy, unchallenged by the right to privacy, will transform the environment of every citizen in the EU into a modern-day panopticon. 'Every object the individual uses…will create a detailed digital record', which will subsequently be used in big data projects to increase the productivity of 'public security efforts'.[39] The citizens of the EU are sleepwalking into a society Mark Weiser warned about: one that will 'make totalitarianism up to now seem like sheerest anarchy'.[40]

If architecture is politics, then the politics of the Commission in policy and rule-making is one of orchestrated silence on the fundamental architectural decisions at stake. In this silence decisions on IoT systems are shaped unrestricted by fundamental rights. The Commission's approach leads to the default recording, collection and retention of data which is generated in the course of the use of electricity or driving a car, as well as the introduction of a range of

[37] Alan F Westin, Privacy and Freedom (New York, Atheneum 1970) 23. He noted attacking the right to privacy is something which is characteristic for both fascism and communism.

[38] Council of the European Union, 'The Stockholm Programme – An open and secure Europe serving and protecting the citizens' (2009) Brussels <https://ec.europa.eu/anti-trafficking/eu-policy/stockholm-programme-open-and-secure-europe-serving-and-protecting-citizens-0_en > accessed 7 June 2018 18.

[39] Future Group, 'Public Security and Technology in Europe: Moving Forward' (Concept paper on the European strategy to transform Public security organisations in a Connected World, Portugal 2007) <http://bit.ly/PqvWIJ> accessed 17 August 2012 8.

[40] Mark Weiser, The Computer for the 21st Century (Scientific American 1991) 25.

vulnerable sensors which can be exploited and turned against citizens. A standard data dispossession regime on these aspects of citizens' lives is the exact opposite of what one would understand as the effective protection of the right to privacy. The collection of data does not serve the right to privacy, especially not if this collection is followed by central storage on servers outside the control of the data subject. The Commission received from internal as well as external sources, time and again, information on how to design both the smart meter and eCall in ways that would respect the right to privacy. It has wilfully ignored this input, leading to a legal vacuum in which architectural choices follow the logic of data dispossession-by-design.

The Commission, of all parties involved, is best placed to turn this development around. It must secure full respect for the right to privacy in pursuance to IoT policy in all its facets if it sincerely desires to stop contributing to the furnishing of its Member States with a technological infrastructure which can be turned into a national or transnational surveillance tool. The Commission plays an important role throughout the policy and rule-making process in which it has the power and duty to guard the fundamental right to privacy. The involuntary systematic recording and collection of data falls under the scope of the right to private life as confirmed in the case law of the ECtHR and the CJEU. The recording and collection of data also falls under data protection legislation as attested to in the GDPR. The rules stemming from Article 7, 8 and 52 of the Charter, as well as the GDPR impose a duty on the legislature to consider the architectural choices at stake. Remaining silent on the architecture of IoT systems and providing merely vague instructions do not meet the specificity principle or the requirement of foreseeability. The architectural choices of the legislature should be guided by the proportionality principle. The relationship between the architectural choices and the surveillance and control potential which can be exploited against citizens, make the application of the necessity test of particular importance: in the context of mandatory IoT systems it allows to 'smoke out unacceptable motives'.[41] A correct application of the proportionality principle, in which the societal implications of the forced installation of IoT systems are taken into consideration, demands that the pursued design avoids or minimises the (risks to) interference with the right to privacy. These choices should ideally result in architectural safeguards which secure the respect for the right to private life and the home and prevent third parties from arbitrarily interfering with citizens' lives. These architectural safeguards can be considered essential elements of design and should have been established by the Commission in the impact assessments prior to the legislative proposal on smart meters and eCall. These essential elements should be adopted in the proposal, and it should be clear for the Council and the EP what is at stake before the relevant legislation is passed. The legislature might then decide against the mandatory nature of the installation.

The architecture of IoT systems should concern all relevant EU institutions if democracy and fundamental rights are not mere slogans in the EU. Deploying surveillance devices on a massive scale which provide public access to private data is typical for totalitarian regimes to

[41] Brems and Lavrysen (n 1) 147.

which the ECHR was a reaction in the first place.[42] This is not to say that the parties which support an all-pervasive vision of the IoT have any political aspirations as such. Totalitarian regimes, nevertheless, share traits with corporations in their attempt to impose a certain vision against people's will, to the extent that they seek to control the feelings, desires and opinions of their respective citizens and customers.[43] The Commission's rhetoric on the importance of privacy and trust for the uptake of the IoT deserves severe criticism given the silent imposition of these systems. The obligation to take on IoT in one's private sphere bears striking similarity with the features going against the essence of democratic justice as conceived by Shapiro: 'it is unnecessary, it is not usually entered into voluntarily, it is hard or impossible to escape, it is both a-symmetrical and non-self-liquidating, and it has effects that permeate through the social world.'[44] The phenomenon he described was slavery.

Ultimately, the answer to be given to the question how the Commission interprets and applies the right to privacy in the policy and rule-making process concerning IoT systems is fairly short. It does not.

[42] Alan F Westin, Privacy and Freedom (New York, Atheneum 1970) 23.

[43] John Dewey, Freedom and culture (London, George Allen and Unwin Ltd 1940) 10.

[44] Ian Shapiro, Democratic Justice (Yale University Press, 1999) 46.